

**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION**

**IN RE: NUMOTION DATA INCIDENT
LITIGATION**

)
)
)
)
)
Case No. 3:24-cv-00545

Judge Aleta A. Trauger

MEMORANDUM

Before the court is the Motion to Dismiss Plaintiffs’ Consolidated Complaint (Doc. No. 28), filed by defendant United Seating and Mobility, LLC d/b/a Numotion (“Numotion”). The motion seeks dismissal of the plaintiffs’ claims under Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure. For the reasons set forth herein, the motion will be granted in part and denied in part.

I. BACKGROUND

This case arises from a cyberattack by a third party (the “Data Incident” or “Data Breach”) on defendant Numotion’s network systems, in which hackers accessed and stole the plaintiffs’ highly sensitive personally identifying information—allegedly as a result of Numotion’s negligence in maintaining the security of its data systems. In June 2024, the court consolidated two related cases bringing claims based on the same incident, and the plaintiffs filed a Consolidated Class Action Complaint (“Consolidated Complaint”) (Doc. No. 23) in July 2024.

As alleged therein, defendant Numotion provides products and services to help individuals with mobility limitations. (Doc. No. 23 ¶ 2.) It is a limited liability company headquartered in Brentwood, Tennessee. (*Id.* ¶ 14.) It has over 150 locations throughout the country and more than 3,000 employees, and it serves more than 300,000 customers. (*Id.* ¶ 20.)

To receive products or services from Numotion, or to be employed by Numotion, the plaintiffs and putative class members were required to provide it personally identifying information (“PII”), including names, passport or driver’s license numbers, dates of birth, and Social Security numbers. Clients also provided protected health information (“PHI,” and, collectively with PII, “Private Information”), including medical equipment information, medical treatment and diagnosis information, and health insurance information. (*Id.* ¶ 3.) The plaintiffs and putative class members did in fact turn over such Private Information to Numotion. (*Id.* ¶ 21.) The plaintiffs allege that Numotion had a common law duty to “adopt reasonable measures” to protect their Private Information from disclosure to unauthorized third parties. (*Id.* ¶ 4.) The plaintiffs allege in addition that Numotion knew or should have known of the risk of a cyberattack (*id.* ¶¶ 57–75); failed to undertake minimally protective measures, such as encrypting Private Information and deleting Private Information once it was no longer needed (*id.* ¶ 44); failed to comply with various federal rules and guidelines for safeguarding electronic forms of medical information (*id.* ¶¶ 76–96); and failed to comply with industry standards (*id.* ¶¶ 97–101).

The named plaintiffs are Shaun Ducrepin, a Minnesota resident and citizen, and Dulcie Walker, a resident and citizen of Arkansas. (*Id.* ¶¶ 12, 13.) Ducrepin was formerly employed by Numotion, and Walker was a customer. Both provided Private Information to Numotion, and both were victims of the Data Incident. (*Id.* ¶¶ 12, 13.)

Specifically, between February 29 and March 2, 2024, the “notorious criminal ransomware group known as Black Basta” accessed Numotion’s “network systems” and extracted and stole the plaintiffs’ and putative class members’ Private Information. (*Id.* ¶ 1.) The plaintiffs allege that Black Basta was able to obtain their Private Information because Numotion breached its duty to safeguard it. (*Id.* ¶ 5.)

Numotion learned about the data breach on March 2, 2024, and it began notifying the plaintiffs and class members about it on April 15, 2024. (*Id.* ¶ 7.) The plaintiffs subsequently discovered that Black Basta “published” the stolen Private Information on its dark web page where, as of July 9, 2024, it had been viewed over 10,000 times. (*Id.* ¶ 9.)

The plaintiffs assert that they face a “lifetime risk of identity theft due to the nature of the Private Information stolen and now disseminated” and that they have incurred injuries arising from the Data Incident in multiple ways. (*Id.* ¶¶ 10, 11.) Specifically, they claim that they, or putative class members, have suffered:

(i) actual identity theft, and the imminent risk thereof; (ii) the lost or diminished value of their Private Information; (iii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) out-of-pocket expenses and lost opportunity costs to mitigate the Data Breach’s consequences, including lost time; (v) loss of privacy, including through the publication and dissemination of their Private Information on the Dark Web; (vi) loss of the benefit of their bargain with Defendant; and (vi) emotional distress associated with the loss of control over their highly sensitive Private Information and attendant, certain risk of identity theft and fraud.

(*Id.* ¶ 11.)

Based on these general allegations,¹ the Consolidated Complaint asserts causes of action on behalf of the named plaintiffs and a putative nationwide class for: (1) negligence; (2) negligence *per se*; (3) breach of implied contract; (4) breach of confidence; (5) unjust enrichment; (6) invasion of privacy; and (7) bailment. (*Id.* ¶ 13; *see also id.* at 50–66.)

In response to the Consolidated Complaint, Numotion filed its Motion to Dismiss all claims asserted therein based on the plaintiffs’ lack of standing and, alternatively, their failure to state a claim for which relief may be granted. (Doc. No. 28.) The motion is supported by a Memorandum

¹ The more specific allegations supporting the plaintiffs’ claims are detailed in the context of addressing the arguments in support of (and opposition to) the Motion to Dismiss.

of Law. (Doc. No. 29.) The plaintiffs filed a Response in opposition to the Motion to Dismiss (Doc. No. 31), and the defendant filed a Reply (Doc. No. 32).

II. RULE 12(b)(1)

A. Standard of Review

Federal Rule of Civil Procedure 12(b)(1) provides for dismissal of a complaint for lack of subject matter jurisdiction. Without subject matter jurisdiction, a federal court lacks authority to hear a case. *Klepsky v. United Parcel Serv., Inc.*, 489 F.3d 264, 268 (6th Cir. 2007). “Motions to dismiss for lack of subject matter jurisdiction fall into two general categories: facial attacks and factual attacks.” *United States v. Ritchie*, 15 F.3d 592, 598 (6th Cir. 1994).

A factual attack is a “challenge to the factual existence of subject matter jurisdiction,” and no “presumptive truthfulness applies to the factual allegations.” *Id.* (citation omitted). A facial attack, like that brought here, “questions merely the sufficiency of the pleading.” *Rote v. Zel Custom Mfg. LLC*, 816 F.3d 383, 387 (6th Cir. 2016) (citation and quotation marks omitted). To survive a facial attack, the complaint must contain a “short and plain statement of the grounds” for jurisdiction. *Id.*

B. Standing Principles

Article III of the Constitution limits the jurisdiction of the federal courts to actual cases or controversies. U.S. Const. art. III, § 2. An essential component of the case-or-controversy requirement is the doctrine of standing, which “limits the category of litigants empowered to maintain a lawsuit in federal court to [those who] seek redress for a legal wrong.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). To establish Article III standing, a plaintiff must show “(i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief.” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021) (citing *Lujan v. Defs. of*

Wildlife, 504 U.S. 555, 560–61 (1992)). If any one of these elements is missing, “there is no case or controversy for the federal court to resolve.” *Id.* (quoting *Casillas v. Madison Ave. Assocs.*, 926 F.3d 329, 333 (7th Cir. 2019) (Barrett, J.)). The party invoking federal jurisdiction has the burden of showing that it has standing. *Id.* at 430–31.

C. Discussion

Numotion argues that the plaintiffs’ allegations fail to establish standing because they have not alleged an injury in fact, harm that is “fairly traceable to the challenged action,” or a harm that is “redressable by a favorable ruling.” (Doc. No. 29 at 10 (citing *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010)).)

1. Injury in Fact

As set forth above, the plaintiffs assert that they suffered injury in the form of: (1) identity theft or the “imminent risk” of identity theft; (2) the diminished value of their Private Information; (3) costs associated with actual identity theft; (4) lost time; (5) present and future mitigation costs incurred in dealing with the imminent risk of identity theft and the unauthorized use of their data; (6) loss of privacy; (7) loss of the benefit of their bargain with Numotion; and (8) emotional distress associated with the theft of their data and the risk of identity theft.

The court notes as an initial matter, however, that the named plaintiffs themselves do not allege that they personally experienced identity theft or that they have personally incurred out-of-pocket expenses in dealing with the threat of identity theft. At this juncture, while it is likely that some putative class member has suffered identity theft, no party presently before the court alleges that he or she suffered identity theft or incurred out-of-pocket expenses in order to mitigate actual or potential identity theft. For an injury in fact to be “concrete” and “particularized,” it “must affect the plaintiff in a personal and individual way.” *Spokeo*, 578 U.S. at 339; *see also Fox v. Saginaw Cnty.*, 67 F.4th 284, 294 (6th Cir. 2023) (holding that plaintiffs pursuing a class action “must allege

an individual injury; they cannot piggyback off the injuries ‘suffered by other, unidentified members of the class’” (quoting *Warth v. Seldin*, 422 U.S. 490, 502 (1975)). In other words, the plaintiffs cannot establish injury in fact based on speculation that putative class members have suffered identity theft or incurred out-of-pocket costs as a result of the Data Incident.

As for the actual injuries that the plaintiffs themselves allegedly incurred, the defendant argues that the risk of identity theft or fraud—*i.e.*, the risk of future harm—does not qualify as an injury in fact. And, according to the defendants, a “large majority” of district courts, following the Supreme Court’s decision in *TransUnion LLC v. Ramirez*, have held that plaintiffs in data breach cases lack standing where they do not allege any out-of-pocket expenses or actual identity theft. (Doc. No. 29 at 12 (collecting cases).) Numotion also asserts that the Sixth Circuit’s contrary conclusion in *Galaria v. Nationwide Mutual Insurance Co.*, 663 F. App’x 384 (6th Cir. 2016), an unreported case that predates *TransUnion*, has been abrogated.

In *Galaria*, the plaintiffs—like the plaintiffs here—brought a putative class action after hackers breached the defendant’s computer network and stole the plaintiffs’ PII, including names, dates of birth, Social Security numbers, driver’s license numbers, and so forth. The district court dismissed the plaintiffs’ negligence and bailment claims for lack of Article III standing, but the Sixth Circuit reversed, finding that the plaintiffs’ “allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, [we]re sufficient to establish a cognizable Article III injury at the pleading stage of the litigation.” *Galaria*, 663 F. App’x at 388.

In reaching that conclusion, the court expressly recognized the Supreme Court’s holdings that, “[t]o establish injury in fact, a plaintiff must show that he or she suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Id.* (quoting *Spokeo*, 578 U.S. at 339). The court also noted that,

when a plaintiff's standing is based on an imminent injury, the “‘threatened injury must be *certainly impending* to constitute injury in fact,’ and that ‘[a]llegations of *possible* future injury’ are not sufficient.” *Id.* (quoting *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013)) (emphasis in original). The Sixth Circuit also noted, however, that the Supreme Court has “found standing based on a ‘substantial risk’ that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm,” even where it is not “literally certain the harms they identify will come about.” *Id.* (quoting *Clapper*, 568 U.S. at 414 n.5 (collecting cases)).

Scrutinizing the pleadings before it under that exacting standard, the Sixth Circuit held in *Galaria* that the plaintiffs’ allegations related to the data breach were sufficient to establish standing, because, although none had experienced identity theft, they alleged that their personal data was actually in the hands of criminals. The theft of their data therefore placed them at a substantial risk of identity theft, “beyond the speculative allegations of ‘possible future injury’ or ‘objectively reasonable likelihood’ of injury that the Supreme Court has explained are insufficient.” *Id.* (quoting *Clapper*, 568 U.S. at 410). Although it was not “literally certain” that the plaintiffs would experience identity theft or the misuse of their data by criminals, there was a “sufficiently substantial risk of harm that incurring mitigation costs is reasonable.” *Id.* Moreover, because the plaintiffs knew their data had been stolen, the court found that it would be “unreasonable to expect [them] to wait for actual misuse . . . before taking steps to ensure their own personal and financial security”—particularly because the defendant recommended taking those steps. *Id.*

The Sixth Circuit has not revisited the issues raised in *Galaria* since *TransUnion*, but a few district courts within this circuit have construed *TransUnion* as “cast[ing] some doubt on the continued viability of *Galaria*,” while also recognizing that the cases are factually distinguishable

and that *Galaria* remains, at the very least, persuasive until and unless the Sixth Circuit revisits the issue. *Brickman v. Maximus*, No. 2:21-cv-03822-MHW-KAJ, 2022 WL 16836186, at *3, *4 (S.D. Ohio May 2, 2022); *see also Brooks v. Peoples Bank*, 732 F. Supp. 3d 765, 775 (S.D. Ohio 2024) (recognizing that *TransUnion* “may have modified the standard for assessing whether a future harm constitutes an Article III injury-in-fact. . . . But as this Court has already said, that is a question for the Sixth Circuit to decide.” (citing *Brickman*, 2022 WL 16836186, at *3–4)); *Kingen v. Warner Norcross + Judd LLP*, No. 1:22-cv-01126, 2023 WL 11965363, at *2 (W.D. Mich. Oct. 5, 2023) (“*TransUnion* seems to reign [sic] in *Galaria*’s future substantial risk of injury standard. In particular, future risk of injury cannot be too speculative; and in some cases, *TransUnion* may require publication to a third party and/or actual knowledge of the harm.”), *reconsideration denied, motion to certify appeal granted*, No. 1:22-cv-1126, 2023 WL 11960672 (W.D. Mich. Nov. 29, 2023). Others, however, have found no real conflict between the cases. *See, e.g., Haney v. Charter Foods N., LLC*, No. 2:23-cv-46, 2024 WL 4054361, at *4 (E.D. Tenn. Aug. 28, 2024) (“*Galaria* is consistent with *TransUnion* and still good law.”); *Lochridge v. Quality Temp. Servs., Inc.*, No. 22-cv-12086, 2023 WL 4303577, at *4 (E.D. Mich. June 30, 2023) (“Defendant argues that, following the Supreme Court’s decision in *TransUnion*, the holding of *Galaria* is no longer valid. The court disagrees.” (internal record citation omitted)); *Bowen v. Paxton Media Grp., LLC*, No. 5:21-CV-00143-GNS, 2022 WL 4110319, at *4 (W.D. Ky. Sept. 8, 2022) (rejecting the defendant’s contention that *Galaria* had been “superseded” by *TransUnion*, stating: “*TransUnion* did not foreclose the possibility of a risk of future harm giving rise to Article III standing, instead creating a two-part test to determine when the risk of harm gives rise to Article III standing when: (1) there is material risk of concrete harm; and (2) plaintiffs can demonstrate

“some other injury” they suffered stemming from this risk.” (quoting *TransUnion*, 594 U.S. at 437)).

TransUnion does not invalidate *Galaria*. Notably, because the facts as alleged here are virtually identical to those in *Galaria*, its conclusions are all the more persuasive. As in *Galaria*, the plaintiffs in this case allege that the defendant’s computer servers were accessed by “notorious” criminals and that this breach put them and putative class members at substantial risk of identity theft and fraud. (Doc. No. 1 ¶¶ 1, 114, 181.) They allege that they and putative class members have taken concrete measures to protect themselves from future harm. (*Id.* ¶¶ 110, 126–27, 136, 161.) Numotion itself recommended that they take many of these steps in the letters notifying them of the Data Incident. (*See* Doc. No. 23-1.) The plaintiffs, in other words, have alleged precisely the type of facts that the Sixth Circuit found were sufficient to plead an Article III injury in fact in *Galaria*:

Here, Plaintiffs’ allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation. Plaintiffs allege that the theft of their personal data places them at a continuing, increased risk of fraud and identity theft beyond the speculative allegations of ‘possible future injury’ or ‘objectively reasonable likelihood’ of injury that the Supreme Court has explained are insufficient. There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals.

Galaria, 663 F. App’x at 388.

In addition, *Galaria* did not address a claim for breach of implied contract. The plaintiffs here, as discussed below, adequately allege the existence of an implied contract and damages in the form of deprivation of the benefit of the (implied) bargain. The Sixth Circuit has recognized that a plaintiff’s loss of the benefit of her bargain with the defendant is a cognizable injury in fact. *Springer v. Cleveland Clinic Emp. Health Plan Total Care*, 900 F.3d 284, 287 (6th Cir. 2018).

The court finds that the plaintiffs have adequately alleged injury in fact for purposes of establishing standing.

2. Causation

Having cleared the injury-in-fact hurdle, the plaintiffs must also establish that the injury was “likely caused by the defendant.” *TransUnion*, 594 U.S. at 423. The causation element, however, is not synonymous with proximate cause. *Galaria*, 663 F. App’x at 390. Rather, a plaintiff’s injury must be “fairly traceable to the conduct being challenged.” *Id.* (quoting *Wittman v. Personhuballah*, 578 U.S. 539, 543 (2016)). The court found that element satisfied in *Galaria*, where the plaintiffs alleged that the defendant’s failure to secure the sensitive personal information entrusted to it allowed the hackers to access the plaintiffs’ data. Although the hackers were obviously the direct cause of the injury, the defendant’s purportedly lax security was the “but for” cause of the cyberattack. *See id.* (“These allegations meet the threshold for Article III traceability, which requires more than speculative but less than but-for causation.” (internal quotation marks and citation omitted)).

So, too, in this case. The plaintiffs allege that the defendant’s lax security measures—in particular, the failure to encrypt Private Information—enabled the criminal third parties to break into the system and access the information. The plaintiffs have sufficiently alleged causation for standing purposes.

3. Redressability

A plaintiff must show that the alleged injury “is likely to be redressed by a favorable judicial decision.” *Wittman*, 578 U.S. at 544 (citation omitted). The plaintiffs seek compensatory damages and other monetary remedies, which would redress their financial harms. (*See* Doc. No. 1 at 66.) *Accord Galaria*, 663 F. App’x at 391 (“Plaintiffs seek compensatory damages for their injuries, and a favorable verdict would provide redress.”). The plaintiffs also seek a declaration

and an injunction requiring the defendant to provide credit and identity-theft monitoring and to strengthen its security protocols. They have plausibly alleged an injury in fact based on a substantial risk of future harm, and an injunction would redress that injury. *Accord TransUnion*, 594 U.S. at 435 (“As this Court has recognized, a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial.”).

The plaintiffs, in sum, have adequately alleged facts establishing Article III standing. The Consolidated Complaint is not subject to dismissal for lack of subject matter jurisdiction under Rule 12(b)(1).

III. RULE 12(b)(6)

A. Standard of Review

The defendant’s motion also seeks dismissal of the Consolidated Complaint based on Rule 12(b)(6) of the Federal Rules of Civil Procedure. A motion to dismiss under Rule 12(b)(6) tests the legal sufficiency of the complaint. *RMI Titanium Co. v. Westinghouse Elec. Corp.*, 78 F.3d 1125, 1134 (6th Cir. 1996). Such a motion is properly granted if the plaintiff has “fail[ed] to state a claim upon which relief can be granted.” Fed. R. Civ. P. 12(b)(6); *Marvaso v. Sanchez*, 971 F.3d 599, 605 (6th Cir. 2020). To survive a motion to dismiss, a complaint must allege facts that, if accepted as true, are sufficient to state a claim to relief that is plausible on its face. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–57 (2007); *see also* Fed. R. Civ. P. 8(a)(2). A complaint has “facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556). The complaint need not contain “detailed factual allegations,” but it must contain more than “labels and conclusions” or “a formulaic recitation of the elements of a cause of action.” *Twombly*, 550 U.S. at 555 (2007). A complaint that “tenders

‘naked assertions’ devoid of ‘further factual enhancement’” will not suffice. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 557).

In ruling on a motion to dismiss under Rule 12(b)(6), the court must “construe the complaint in the light most favorable to the plaintiff, accept all well-pleaded factual allegations in the complaint as true, and draw all reasonable inferences in favor of the plaintiff.” *Courtright v. City of Battle Creek*, 839 F.3d 513, 518 (6th Cir. 2016).

B. Discussion

Numotion argues that many of the plaintiffs’ claims, including their negligence, negligence *per se*,² breach of implied contract, and breach of confidence claims require them to plead cognizable damages and that their failure to do so requires dismissal of these claims. They also assert that the breach of implied contract, breach of confidence, unjust enrichment, invasion of privacy, and bailment claims must be dismissed for failure to state claims for which relief may be granted. The court addresses this latter argument first.

1. Choice of Law

Neither party raises the issue of choice of law. The defendant presumes that Tennessee law applies, and the plaintiffs do not argue to the contrary. “A federal court sitting in diversity ordinarily must follow the choice-of-law rules of the State in which it sits.” *Atl. Marine Constr. Co. v. U.S. Dist. Ct.*, 571 U.S. 49, 66 (2013) (citation omitted). Tennessee applies the “most significant relationship test” to tort claims, which requires consideration of several factors, including (1) the place where the injury occurred; (2) the place where the conduct causing the injury occurred; (3) the domicile, residence, nationality, place of incorporation and place of

² The defendant does not separately address the negligence *per se* claim but generally addresses the negligence claims together, as does the court.

business of the parties; and (4) the place where the relationship, if any, between the parties is centered. *Hataway v. McKinley*, 830 S.W.2d 53, 59 (Tenn. 1992). These factors are “evaluated according to their relative importance with respect to the particular issue.” *Id.* In personal injury cases, application of these factors generally means that the law of the state where the injury occurred applies, unless some other state has a more significant relationship to the litigation. *Id.* A contract, under Tennessee law, is “presumed to be made with reference to the law of the place where it was entered into *unless it appears it was entered into in good faith with reference to the law of some other state.*” *Williams v. Smith*, 465 S.W.3d 150, 154 (Tenn. Ct. App. 2014) (quoting *Ohio Cas. Ins. Co. v. Travelers Indem. Co.*, 493 S.W.2d 465, 467 (Tenn. 1973)) (emphasis in original).

At this juncture, the court will apply Tennessee law to the tort claims, both because Tennessee appears to be the state with the most significant relationship to the plaintiffs’ claims and because the plaintiffs do not argue to the contrary. While the proposed class is nationwide, meaning that the named plaintiffs’ and the putative class members’ domiciles vary and that the alleged injuries occurred in different states,³ the data breach occurred in Tennessee, and the defendant is based in Tennessee. Similarly, for the contract-based claims, although there is no written contract, any contractual duties were undertaken by a Tennessee-based business, and the alleged breach-of-implied-contract claim relies on actions taken in Tennessee. The court, therefore, will apply Tennessee law to the breach of implied contract claim as well.

³ The named plaintiffs are citizens of Arkansas and Minnesota. (Doc. No. 23 ¶¶ 12–13.)

2. Breach of Implied Contract

A contract implied in fact⁴ (“implied contract”) “is similar to an express contract, in that it ‘arises under circumstances which show mutual intent or assent to contract,’ and ‘it must be supported by . . . consideration and lawful purpose.’” *ICG Link, Inc. v. Steen*, 363 S.W.3d 533, 543 (Tenn. Ct. App. 2011) (quoting *Jones v. LeMoyne–Owen Coll.*, 308 S.W.3d 894, 905 (Tenn. Ct. App. 2009)). “The primary difference between the two is the manner in which the parties express their assent.” *Jones*, 308 S.W.3d at 905 (citing *Thompson v. Hensley*, 136 S.W.3d 925, 930 (Tenn. Ct. App. 2003)). “In an express contract, the parties assent to the terms of the contract by means of words, writings, or some other mode of expression. . . . In a contract implied in fact, the conduct of the parties and the surrounding circumstances show mutual assent to the terms of the contract.” *Id.* (quoting *Thompson*, 136 S.W.3d at 930) (alteration in original).

The plaintiffs allege that Numotion required them to “provide and entrust their Private Information as a condition of obtaining healthcare products and services and/or employment” from Numotion and, at the same time, impliedly agreed to “safeguard and protect such Private Information and to timely and accurately notify Plaintiffs and Class Members if and when their Private Information was . . . compromised.” (Doc. No. 23 ¶¶ 238–39.) The plaintiffs allegedly relied on this implied agreement as a “material aspect” of their contractual relationship with the defendant, and they “reasonably believed and expected that Defendant’s data security practices

⁴ The Tennessee Supreme Court has distinguished between “contracts implied in fact and contracts implied in law.” *Paschall’s, Inc. v. Dozier*, 407 S.W.2d 150, 153 (Tenn. 1966). Regarding the latter, the court stated that “[a]ctions brought upon theories of unjust enrichment, quasi contract, contracts implied in law, and quantum meruit are essentially the same.” *Id.* at 154; see also *Freeman Indus., LLC v. Eastman Chem. Co.*, 172 S.W.3d 512, 524–25 (Tenn. 2005) (“Courts may impose a contract implied in law where no contract exists under various quasi contractual theories, including unjust enrichment.”). Because the plaintiffs here bring a separate claim for unjust enrichment, discussed below, the court presumes that their claim for breach of implied contract is a claim based on a contract implied in fact.

complied with industry standards and relevant laws and regulations.” (*Id.* ¶ 246.) The plaintiffs further allege that a meeting of the minds occurred with respect to the defendant’s obligation to safeguard their Private Information, which is further substantiated by the existence of “multiple documents” that embody and memorialize the defendant’s contractual obligation, including Numotion’s Notice of Privacy Practices and Employee Privacy Policy. (*Id.* ¶ 244.) The plaintiffs allege that they performed their obligations under the implied contracts when they provided their Private Information and purchased services from, or provided labor to, Numotion and that Numotion unilaterally breached the implied contract when it failed to “implement even minimally reasonable logging and monitoring systems, among other safeguards, and thus allowed Plaintiffs’ and Class Members’ data to be disclosed to criminal actors bent on identity theft, fraud, and extortion.” (*Id.* ¶¶ 249–50.)

Numotion argues that the Consolidated Complaint fails to adequately allege facts showing a meeting of the minds or consideration. Rather, according to Numotion, the plaintiffs “allege that Numotion had pre-existing obligations to protect their data . . . , which cannot form the basis for consideration of an implied contract.” (Doc. No. 29 at 23.) It contends that consideration exists “when the promisee does something that it is under no legal obligation to do” and that, based on the plaintiffs’ own allegations, Numotion was legally obligated by various federal statutes and regulations to safeguard the plaintiff’s Private Information. (*Id.* (citing *GuestHouse Int’l, LLC v. Shoney’s N. Am. Corp.*, 330 S.W.3d 166, 188 (Tenn. Ct. App. 2010)).)

In response, the plaintiffs point to numerous cases holding that allegations of the type made here can support both the mutual assent and consideration elements of implied contract claims, and they urge this court to follow this trend. *See, e.g., Clemens v. ExecuPharm, Inc.*, 678 F. Supp. 3d 629, 638 (E.D. Pa. 2023); *Rodriguez v. Mena Hosp. Comm’n*, No. 2:23-cv-2002, 2023 WL

7198441, at *7 (W.D. Ark. Nov. 1, 2023); *Farmer v. Humana, Inc.*, 582 F. Supp. 3d 1176, 1187 (M.D. Fla. 2022); *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 750–51 (S.D.N.Y. 2017). *But see Enslin v. Coca-Cola Co.*, No. 2:14-cv-06476, 2017 WL 1190979, at *14 (E.D. Pa. Mar. 31, 2017) (noting that “both the Pennsylvania Superior Court and the Third Circuit, applying Pennsylvania law, have rejected the notion that when an employee provides an employer with personal information, an implied contract arises that obligates the employer to use reasonable measures to safeguard that information” (citing *Longenecker–Wells v. Benecard Servs. Inc.*, 658 F. App’x 659, 662 (3d Cir. 2016))).

The Tennessee Supreme Court has recognized that an implied contract of confidentiality can arise between a physician and a patient when a patient compensates a physician for medical treatment, which a physician may breach when he releases confidential information about the patient without his permission. *Givens v. Mullikin ex rel. Est. of McElwaney*, 75 S.W.3d 383, 407 (Tenn. 2002). Similarly, several courts within the Sixth Circuit, in data breach cases, have held that “an implied contract is formed between an employer and employee when employees are required to provide personal information to their employer as a condition of their employment, and the resulting implied contract requires the employer to take reasonable steps to protect the employees’ information.” *Haney*, 2024 WL 4054361, at *11 (citing *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 821 (E.D. Ky. 2019) (holding that the plaintiffs stated a claim for breach of implied contract where they alleged that they had to provide personal information “as a condition of their employment” and that the defendant “implicitly agreed to safeguard that information”); *Bowen*, 2022 WL 4110319, at *7 (same)).

More than one court has observed that “it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of . . . sensitive personal information would not

imply the recipient's assent to protect [the] information sufficiently." *Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1195 (D. Nev. 2022) (quoting *Castillo v. Seagate Tech., LLC*, No. 16-cv-01958, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016)). In accordance with a clear majority of the courts that have considered the issue, the court finds that the plaintiffs adequately allege the existence of an implied agreement, a meeting of the minds, and consideration to support the existence of an implied contract to engage in reasonable means to protect the plaintiffs' Private Information.

3. "Breach of Confidence"

Count IV of the Consolidated Complaint sets forth a claim for "Breach of Confidence." (See Doc. No. 23 at 59.) The claim is based on allegations that Numotion collected the plaintiffs' confidential and sensitive information with "explicit and implicit understandings that Defendant would protect . . . the Private Information," and Numotion failed to prevent or avoid the Data Incident. (*Id.* ¶¶ 263–67.) As a result of Numotion's failure to follow "industry standard information security practices," the plaintiffs' Private Information was "disclosed [to] and misappropriated [by] unauthorized third parties." (*Id.* ¶ 268.)

No Tennessee court, to this court's knowledge, has recognized a cause of action for "breach of confidence," but "Tennessee has long recognized a cause of action for breach of confidential relationship." *Heflin v. Iberiabank Corp.*, 571 S.W.3d 727, 736 (Tenn. Ct. App. 2018) (citing *Given*, 75 S.W.3d at 410). "A confidential relationship is one in which 'confidence is placed by one in the other and the recipient of that confidence is the dominant personality, with ability, because of that confidence[,] to influence and exercise dominion and control over the weaker or dominated party.'" *Id.* (quoting *Givens*, 75 S.W.3d at 410). The elements of a claim for breach of confidential relationship are:

(1) the defendant was in a position to influence or control the plaintiff; (2) the defendant used the confidences given to him or her to obtain some benefit from, or advantage over, the plaintiff; and (3) the plaintiff, as the dominated party in the relationship, suffered some detriment at the hands of the defendant.

Id. (quoting *Givens*, 75 S.W.3d at 410); *see also Kelly v. Allen*, 558 S.W.2d 845, 848 (Tenn. 1977)

(“[T]here must be a showing that there were present the elements of dominion and control by the stronger over the weaker.”).

The plaintiffs’ arguments to the contrary notwithstanding, the Consolidated Complaint does not remotely allege facts suggesting that the plaintiffs were in a confidential relationship with Numotion or that Numotion exploited such a relationship by exercising undue influence over the plaintiffs. There is no suggestion that the plaintiffs’ will was somehow overcome or that the defendant, as the dominating party, exercised its will over the plaintiffs to obtain confidences and then used those confidences to “obtain some benefit from, or advantage over, the plaintiff[s].” *Heflin*, 571 S.W.3d at 736.

The plaintiffs, in short, do not allege facts that would establish the elements of a claim for breach of a confidential relationship, and Tennessee does not recognize a cause of action for a “breach of confidence.” This claim will be dismissed.

4. *Unjust Enrichment*

In Tennessee, the elements of unjust enrichment are

1) a benefit conferred upon the defendant by the plaintiff; 2) appreciation by the defendant of such benefit; and 3) acceptance of such benefit under such circumstances that it would be inequitable for him to retain the benefit without payment of the value thereof.

Freeman Indus., 172 S.W.3d at 525 (quoting *Paschall’s, Inc.*, 407 S.W.2d at 155) (brackets and internal quotation marks omitted). “The most significant requirement of an unjust enrichment claim is that the benefit to the defendant be unjust.” *Id.*

The plaintiffs here assert that they “conferred direct benefits upon Defendant in the form of agreeing to provide their Private Information to Defendant, without which Defendant could not perform the services it provides or pay its employees.” (Doc. No. 23 ¶ 276.) They assert that the defendant “appreciated” these benefits and “should not be allowed to retain the full value of these benefits—specifically, the costs it saved by failing to implement reasonable or adequate data security practices”—and that, if the plaintiffs had known of the inadequacies of the defendant’s data practices, they would never have agreed to entrust their Confidential Information to the defendant. (*Id.* ¶¶ 277–29.)

Numotion argues that the plaintiffs fail to plausibly plead unjust enrichment, because it is clear that plaintiff Ducrepin provided services to the defendant for which he was paid, and plaintiff Walker received services from Numotion for which she paid Numotion, and these exchanges of benefits are “independent from the Personal Information that Numotion had to record in order to effectuate those transactions.” (Doc. No. 29 at 25.) Although the plaintiffs also allege that their Private Information is of “great value to hackers and cybercriminals as it can be used for a variety of unlawful and nefarious purposes” (Doc. No. 23 ¶ 55), the defendant points out that the plaintiffs do not allege that *Numotion* benefitted by allowing the hackers to access the plaintiffs’ Private Information or otherwise used that information for unlawful purposes.

Numerous district courts within the Sixth Circuit have dismissed unjust enrichment claims raised in the data breach context because the plaintiffs’ “personal information does not confer a benefit upon Defendants.” *Haney*, 2024 WL 4054361, at *11; *accord, e.g., Kingen*, 2023 WL 11965363, at *5 (“Other courts have found that it was the third-party hackers—not the defendants—that benefited from a data breach.”), *reconsideration denied, motion to certify appeal granted*, No. 1:22-cv-1126, 2023 WL 11960672 (W.D. Mich. Nov. 29, 2023); *Lochridge*, 2023

WL 4303577, at *7 (same, applying Michigan law); *Tate v. EyeMed Vision Care, LLC*, No. 1:21-cv-36, 2023 WL 6383467, at *8 (S.D. Ohio Sept. 29, 2023) (“[T]his claim is implausible on its face.” (applying Ohio law)).

This court agrees with the majority of district courts in this circuit and finds that the plaintiffs did not confer a benefit upon Numotion by providing their personal data. Moreover, even if they had, they have not alleged facts suggesting it would be inequitable for Numotion to retain the benefit without paying the value thereof, given that it was the hackers—not Numotion—who benefited from the Data Incident. Accordingly, the court will dismiss the claim for unjust enrichment.

5. *Invasion of Privacy*

Tennessee courts recognize two forms of the tort of invasion of privacy: (1) public disclosure of private facts; and (2) intrusion upon seclusion. *See Finley v. Kelly*, 384 F. Supp. 3d 898, 910 (M.D. Tenn. 2019) (collecting cases and discussing both forms of the tort). Because the plaintiffs do not distinguish between them or attempt to make it clear which version they rely on, the court considers the elements of both.

a) *Intrusion Upon Seclusion*

The Tennessee Supreme Court has expressly recognized the tort of intrusion upon seclusion and has defined the cause of action as requiring the plaintiff to show “an intentional, and objectively offensive, interference with his or her interest in solitude or seclusion.” *Givens*, 75 S.W.3d at 411–12 (citing *Restatement (Second) of Torts* § 652B cmt. a). Thus, “[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.” *Id.* at 411 (quoting *Roberts v. Essex Microtel Assocs., II, L.P.*, 46 S.W.3d 205, 211 (Tenn. Ct. App. 2001)).

Here, irrespective of whether Numotion was reckless with respect to its safeguarding of the plaintiffs' Private Information, as the plaintiffs claim, the plaintiffs do not allege that *Numotion* intruded upon their seclusion; Black Basta, a criminal third party, did so. To extend liability to Numotion for Black Basta's intentional criminal intrusion upon the plaintiffs' seclusion would be to extend the tort far beyond what the Tennessee courts have recognized.

b) Public Disclosure of Private Facts

Although the Tennessee Supreme Court has not expressly recognized the tort of public disclosure of private facts, the Tennessee Court of Appeals has. *See Finley*, 384 F. Supp. 3d at 909 (collecting cases). To prevail on a public disclosure claim, the plaintiffs must allege and prove that *the defendant* "gave 'publicity' to a matter concerning plaintiff's private life." *Hoffman v. GC Servs. Ltd. P'ship*, No. 3:08-cv-255, 2010 WL 9113645, at *20 (E.D. Tenn. Mar. 3, 2010) (citing *Beard v. Akzona, Inc.*, 517 F. Supp. 128, 132 (E.D. Tenn. 1981)); *see also Jackson & Assocs., Ltd. v. Christl*, No. 01A019103CV00081, 1991 WL 155687, at *3 (Tenn. Ct. App. Aug. 16, 1991). This version of invasion of privacy is also an intentional tort. *Accord Lineberry v. State Farm Fire & Cas. Co.*, 885 F. Supp. 1095, 1098 (M.D. Tenn. 1995) (Echols, J.) ("This tort is intentional, as it requires that the publisher know that: (1) the matter being revealed is of the kind that would be highly offensive to the reasonable person; and (2) that the information revealed is not of legitimate public concern.").

Setting aside Numotion's other arguments regarding whether Black Basta's posting of the plaintiffs' private information on the dark web qualifies as public disclosure, the fact that the plaintiffs do not allege that *Numotion* published their information is fatal to their claim against Numotion. Again, even assuming that Numotion acted recklessly in failing to safeguard the plaintiffs' Private Information, its recklessness does not give rise to vicarious liability for Black Basta's intentional criminal acts.

The Consolidated Complaint fails to state a colorable invasion of privacy claim against Numotion.

6. *Bailment*

The Tennessee Supreme Court defines bailment as “a delivery of personalty for a particular purpose or on mere deposit, on a contract express or implied; that after the purpose has been fulfilled, it shall be redelivered to the person who delivered it, or otherwise dealt with according to his direction or kept until he reclaims it.” *Akers v. Prime Succession of Tenn., Inc.*, 387 S.W.3d 495, 510 (Tenn. 2012) (quoting *Dispeker v. New S. Hotel Co.*, 373 S.W.2d 904, 908 (Tenn. 1963)). A bailment typically (but not always) involves a contractual relationship, whether actual or implied. *Id.* (citing *Aegis Investigative Grp. v. Metro. Gov’t*, 98 S.W.3d 159, 163 (Tenn. Ct. App. 2002)). “Unlike a sale or gift of personal property, a bailment involves a change in possession but not in title.” *Meade v. Paducah Nissan, LLC*, No. M2021-00563-COA-R3-CV, 2022 WL 2069160, at *4 (Tenn. Ct. App. June 9, 2022) (quoting Bailment, *Black’s Law Dictionary* 162 (9th ed. 2009)).⁵

⁵ According to Black’s Law Dictionary:

A “bailor” is a person who delivers personal property to another as a bailment. A “bailee” is a person who receives personal property from another, and has possession of but not title to the property; a bailee is responsible for keeping the property safe until it is returned to the owner.

A “bailment for hire” is a bailment for which the bailee is compensated, and a “bailment for mutual benefit” is a bailment for which the bailee is compensated and from which the bailor receives some additional benefit, as when one leaves a car with a parking attendant who will also wash the car while it is parked. Moreover, a “gratuitous bailment” is a bailment for which the bailee receives no compensation, as when one borrows a friend’s car; a gratuitous bailee is liable for loss of the property only if the loss is caused by the bailee’s gross negligence.

Black’s Law Dictionary 162.

Citing a case applying Indiana law, the plaintiffs assert that they have adequately alleged all of the necessary elements of both a tort claim and a contract claim for bailment based on the defendant's failure to safeguard their property. (Doc. No. 31 at 23 (citing *Krupa v. TIC Int'l Corp.*, No. 1:22-cv-01951-JRS-MG, 2023 WL 143140, at *5 (S.D. Ind. Jan. 10, 2023)).) In *Krupa*, the court concluded that the plaintiffs had indeed stated a viable bailment claim in a data breach case under circumstances similar to those presented here:

Krupa alleges that TIC held his personal data subject to a shared understanding that it would remain confidential, but that TIC negligently exposed that data to hackers. Krupa needs nothing more to establish a breach of bailment claim. He plausibly alleges that his data is “personal property” that is in TIC’s “exclusive possession” once on TIC’s servers, and that TIC had “accepted” the data in the course of business. Krupa avoids the “exclusive possession” problem . . . because . . . he was unable to manipulate his personal data on TIC’s servers; TIC was in full control.

Krupa, 2023 WL 143140, at *5 (internal citations omitted).

The plaintiffs in the present case have not plausibly (or even implausibly) alleged that their Private Information is in Numotion’s exclusive possession. (See Doc. No. 23 ¶¶ 297–302.) Moreover, aside from *Krupa*, basically every district court that has considered a bailment claim in the context of data breach litigation—including other Indiana federal district courts, as well as courts applying Tennessee law—has rejected the claim for various reasons, but most often because the plaintiffs cannot plausibly allege that the defendant was in *exclusive* possession of their PII, simply given the nature of PII. See, e.g., *Cahill v. Mem’l Heart Inst., LLC*, No. 1:23-cv-168, 2024 WL 4311648, at *14 (E.D. Tenn. Sept. 26, 2024) (“Personal information is intangible and transfer of PII to one party does not limit transfer to another party. Plaintiffs do not plausibly allege they delivered PII to Defendant’s exclusive control, or that they transferred custody of their PII with the expectation that Defendants would deliver it back to them. Plaintiffs fail to state a claim for bailment.”); *Johnson v. Nice Pak Prods., Inc.*, No. 1:23-cv-01734-JMS-CSW, 2024 WL 2845928, at *8 (S.D. Ind. June 5, 2024) (acknowledging *Krupa* and rejecting it because the plaintiffs did not

allege that their PII was in the defendants’ “exclusive possession,” as the plaintiffs remained “free to use or disseminate their PII as they pleased and deliver it to limitless others”); *Galaria v. Nationwide Mut. Ins. Co.*, No. 2:13-cv-118, 2017 WL 4918634, at *2 (S.D. Ohio Oct. 31, 2017) (finding that the plaintiffs failed to state a bailment claim where they “have not alleged that they transferred control or custody of their personal identifiers to Defendant” and instead “retained their personal identifiers and continued to use them throughout the period of the alleged bailment”), *R. & R. adopted*, No. 2:13-cv-118, 2017 WL 6375803 (S.D. Ohio Dec. 13, 2017); *see also McLaughlin v. Taylor Univ.*, No. 1:23-cv-00527-HAB-SLC, 2024 WL 4274848, at *12 (N.D. Ind. Sept. 23, 2024) (“[*Krupa*] is an outlier case. The predominant view across the country is that bailment is not a viable theory in data breach cases.”); *Miller v. NextGen Healthcare, Inc.*, No. 1:23-CV-2043-TWT, 2024 WL 3543433, at *4 (N.D. Ga. July 25, 2024) (“Courts have generally rejected bailment theories against defendants who allegedly did not adequately protect private information from data breaches.”).

This court agrees with the majority of courts deciding this issue. Even assuming that intangible property can be the subject of a bailment, the plaintiffs fail to allege that they transferred *exclusive* possession of their Private Information to the defendant. The Consolidated Complaint, therefore, fails to state a colorable bailment claim.

7. *Damages*

Numotion also argues that the plaintiffs’ negligence and breach of implied contract claims are subject to dismissal because these claims require injury as an element of the cause of action, and the plaintiffs fail to plead a cognizable injury. (Doc. No. 29 at 19–20.) Although the court has found that the plaintiffs have adequately alleged an injury in fact for purposes of establishing standing, whether the Consolidated Complaint “adequately allege[s] compensable damages is a different question.” *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App’x 613, 614 (9th Cir.

2021) (citing *Doe v. Chao*, 540 U.S. 614, 624–25 (2004)); *see also Hicks v. State Farm Fire & Cas. Co.*, 965 F.3d 452, 463 (6th Cir. 2020) (“[A]s the Supreme Court has reminded, ‘one must not confuse weakness on the merits with absence of Article III standing.’” (citing *Ariz. State Legislature v. Ariz. Indep. Redistricting Comm’n*, 576 U.S. 787, 800 (2015))); *Carlsen v. GameStop, Inc.*, 833 F.3d 903, 909 (8th Cir. 2016) (“[I]t is crucial . . . not to conflate Article III’s requirement of injury in fact with a plaintiff’s potential causes of action, for the concepts are not coextensive.” (citation, alteration, and quotation marks omitted)).

In connection with their negligence claims, the plaintiffs allege past injury, for which they seek monetary damages, in the form of: (1) redress for invasion of privacy; (2) diminished value of their Private Information; (3) lost time associated with attempting to mitigate the consequences of the Data Incident; (4) anxiety and emotional distress; and (5) other non-specified economic and non-economic losses. (Doc. No. 23 ¶¶ 220–21, 234–35.) In connection with their breach of implied contract claim, they assert damages in the form of the “loss of benefit of the bargain” with Numotion. (*Id.* ¶ 259.) They also assert that they are at risk of future injury due to the “increased risk to their Private Information,” which they claim “(i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendant’s possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.” (*Id.* ¶¶ 220, 234.) They seek injunctive relief requiring the defendant to take adequate measures to protect their Private Information that remains in Numotion’s possession and to provide credit monitoring services to them and all class members for at least five years, or, alternatively, monetary damages to cover the cost of such monitoring. (*Id.* ¶¶ 174, 222–233, 235–36, 260–61.)

Numotion asserts that time expended to mitigate speculative damages is not compensable; that the alleged diminution in the value of the plaintiffs' Private Information is not a compensable injury; that the mere possibility of being damaged in the future is not compensable; and that damages for emotional distress and anxiety, in the context of negligence claims, are compensable under Tennessee law only for "serious" or "severe" emotional injury. (Doc. No. 29 at 20–22.)

a) Breach of Implied Contract

The plaintiffs allege damages arising from breach of implied contract in the form of the loss of the benefit of the bargain. Specifically, they assert that they were damaged "in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received." (Doc. No. 23 ¶ 254.) They seek monetary damages in that amount, as well as injunctive relief requiring the defendant to, among other things, strengthen its data security and provide adequate and ongoing credit monitoring to all class members. Alternatively, they seek monetary damages to cover future credit monitoring. They specifically allege that:

retail cost of credit monitoring and identity theft monitoring can cost \$200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

(*Id.* ¶ 174.) The plaintiffs do not allege that they have actually incurred the cost of credit monitoring.⁶

⁶ Although the Consolidated Complaint does not expressly allege as much, the "notice" letters attached to the pleading indicate that Numotion offered individuals whose information was stolen "a complimentary one-year membership" in a credit and identity-theft monitoring company, thus apparently obviating the need for any plaintiff to immediately spend money on credit monitoring. (See Doc. No. 23-1, at 2, 6.)

While courts addressing this type of claim have reached conflicting decisions, the general consensus appears to be “that credit monitoring may be compensable where evidence shows that the need for future monitoring is a reasonably certain consequence of the defendant’s breach of duty [T]he monitoring must be reasonable and necessary.” *Greenstein v. Noblr Reciprocal Exch.*, 585 F. Supp. 3d 1220, 1229 (N.D. Cal. 2022) (citations omitted). Thus, for example, in *Greenstein*, future monitoring was not considered either reasonable or necessary, where the type of data stolen (the plaintiff’s and putative class members’ names, driver’s license numbers, and addresses) did not qualify as “highly sensitive personal information” and did not “provide hackers with a clear ability to commit fraud,” as driver’s license numbers “are considered not as sensitive as social security numbers.” *Id.* at 1227. However, the hacking of highly sensitive information, particularly including Social Security numbers and health information, is usually considered to give rise to a sufficiently real and imminent risk of identity theft to warrant monitoring. *Accord, e.g., In re Unite Here Data Sec. Incident Litig.*, No. 24-cv-1565(JSR), 2024 WL 3413942, at *3 (S.D.N.Y. July 15, 2024) (“Because healthcare and personally identifiable information are especially attractive and vulnerable to cyberattacks, the data breach qualifies as a targeted attempt to obtain that data. In such circumstances, it is reasonable to infer the purpose of the attack was to misuse the data.”), *motion to certify appeal denied*, No. 24-cv-1565 (JSR), 2024 WL 4307975 (S.D.N.Y. Sept. 26, 2024).

At this juncture, the court finds that the plaintiffs have adequately pleaded entitlement to benefit of the bargain damages, as well as future damages in the form of the reasonable cost of credit monitoring or an injunction requiring the defendant to provide credit monitoring and to strengthen its security protocols.

b) *Negligence*

The elements of a negligence claim under Tennessee law are: “1) a duty of care owed by the defendant to the plaintiff; 2) conduct falling below the applicable standard of care amounting to a breach of that duty; 3) an injury or loss; 4) causation in fact; and 5) proximate, or legal, cause.” *King v. Anderson Cnty.*, 419 S.W.3d 232, 246 (Tenn. 2013). “No claim for negligence can succeed in the absence of any one of these elements.” *Cox v. M.A. Primary & Urgent Care Clinic*, 313 S.W.3d 240, 259 (Tenn. 2010) (citation omitted)

“An award of damages, which is intended to make a plaintiff whole, compensates the plaintiff for damage or injury caused by a defendant’s wrongful conduct.” *Dedmon v. Steelman*, 535 S.W.3d 431, 437 (Tenn. 2017) (quoting *Meals ex rel. Meals v. Ford Motor Co.*, 417 S.W.3d 414, 419 (Tenn. 2013)). “The party seeking damages has the burden of proving them.” *Id.* (quoting *Overstreet v. Shoney’s, Inc.*, 4 S.W.3d 694, 703 (Tenn. Ct. App. 1999)).

Under Tennessee law, a plaintiff injured by another’s negligence may recover two types of damages: “economic (or pecuniary) damages and non-economic (or personal) damages.” *Dedmon*, 535 S.W.3d at 437 (citing *Meals*, 417 S.W.3d at 419–20). Economic damages, which includes quantifiable expenses such as past and future medical expenses, lost wages, and lost earning potential, “have a monetary value that is readily ascertainable. It is therefore reasonable to require that plaintiffs prove the monetary value of such damages with relative precision.” *Health Cost Controls, Inc. v. Gifford*, 239 S.W.3d 728, 733 (Tenn. 2007). “Non-economic damages include pain and suffering, permanent impairment and/or disfigurement, and loss of enjoyment of life.” *Dedmon*, 535 S.W.3d at 438 (quoting *Meals*, 417 S.W.3d at 420). Such damages are generally “highly subjective and are not susceptible to proof by a specific dollar amount.” *Id.* The question presented here is whether the injuries claimed by the plaintiffs are compensable.

Lost Time

The Ninth Circuit has affirmed a district court’s dismissal of negligence and other claims raised in a data breach claim, finding that, despite having sufficiently alleged injury in fact for standing purposes, the plaintiff’s allegations of “lost time” were not cognizable under Nevada law. *See Pruchnicki*, 845 F. App’x at 614 (“Pruchnicki cites no authority recognizing lost time as a cognizable injury for the purpose of establishing compensable damages. And several district courts in this Circuit have declined to recognize such damages unless accompanied by out-of-pocket expenses.”). District courts within the Ninth Circuit have generally followed suit. *See, e.g., Johnson v. Yuma Reg’l Med. Ctr.*, No. CV-22-01061-PHX-SMB, 2024 WL 4803881, at *3 (D. Ariz. Nov. 15, 2024) (“[T]he majority view is that general allegations of lost time, continued risk to plaintiffs’ personal data, and the danger of future harms are not cognizable injuries for negligence claims.” (collecting cases)); *Quinalty v. FocusIT LLC*, No. CV-23-00207-PHX-JJT, 2024 WL 342454, at *4–5 (D. Ariz. Jan. 30, 2024); *In re Eureka Casino Breach Litig.*, No. 2:23-cv-00276-CDS-BNW, 2024 WL 4253198, at *3 (D. Nev. Sept. 19, 2024); *Gardiner v. Walmart, Inc.*, No. 20-cv-04618-JSW, 2021 WL 4992539, at *5 (N.D. Cal. July 28, 2021).

Outside the Ninth Circuit, district courts have generally concluded that “lost time” allegations may satisfy the injury requirement for data breach negligence claims. *See, e.g., In re: Netgain Tech., LLC*, No. 21-cv-1210 (SRN/LIB), 2022 WL 1810606, at *14 (D. Minn. June 2, 2022) (“Courts have held that damages like monitoring and lost time are cognizable.”); *Baldwin v. Nat’l W. Life Ins. Co.*, No. 2:21-cv-04066-WJE, 2021 WL 4206736, at *3 (W.D. Mo. Sept. 15, 2021) (“[P]urported time and effort monitoring accounts can qualify as an injury to support Plaintiffs’ claims.”).

As noted above, the named plaintiffs in this case do not allege that they have incurred out-of-pocket expenses in response to the Data Incident. Instead, they have spent time “seeking legal advice” and monitoring their accounts. (Doc. No. 23 ¶¶ 126, 136.) As Numotion points out, the plaintiffs have not pointed to any Tennessee case in which damages for “lost time” have been awarded. It is logical to conclude that, if damages for lost time were available under Tennessee law, Tennessee courts would regularly award such damages in, for example, personal injury cases in which the plaintiffs, given the nature of their injuries, may be presumed to have devoted a substantial amount of time to such endeavors as driving to and from doctors’ appointments, sitting in waiting rooms, undergoing medical procedures, making phone calls and writing letters and otherwise dealing with insurance companies, awaiting car repairs, and the like. The court finds it significant that, outside of lost wages and lost earning potential, which are concretely quantifiable and susceptible of direct proof, Tennessee courts have not awarded such damages.

In the absence of Tennessee caselaw awarding such damages, the court finds that the plaintiffs’ allegations of lost time do not establish a compensable injury for negligence.

Invasion of Privacy

As discussed above, the plaintiffs have articulated a stand-alone invasion-of-privacy claim, but the court has found that their allegations fail to state a colorable claim *against Numotion*. For the same reasons, the plaintiffs’ damages in the form of publication of their private data by a third party is not an injury that can be attributable to Numotion.

Diminished Value of Private Information

The plaintiffs assert that Private Information is a “valuable property right” and that their information has substantial value in the marketplace. Although they allege that its value has been diminished on the black market, they do not plausibly allege that they ever intended to sell their

Private Information on the black market or that the loss has impaired their ability to participate in the economic marketplace.

Most courts considering this type of “injury” have concluded that it is not compensable, at least in the absence of plausible allegations that the plaintiffs have lost the ability to sell their information on the black market or that their ability to participate in the marketplace has been impaired. *Accord, e.g., Bonewit v. New-Indy Containerboard LLC*, No. 24-cv-11338-DJC, 2024 WL 4932186, at *5 (D. Mass. Dec. 2, 2024) (“Bonewit relies upon general allegations of PII’s value on the black market, but has not alleged that Bonewit’s PII has lost value in legitimate markets or explained how the hacker’s possession of PII diminishes its value.”); *Quinalty*, 2024 WL 342454, at *4–5 (recognizing that a “plaintiff can establish the diminished value of PII as a cognizable injury if the plaintiff shows a ‘robust market’ for the PII and that the plaintiff has been deprived of the ability to sell personal data on the market,” but finding no cognizable injury in that case because the plaintiff did “not allege she can no longer sell her personal data on the market, nor does she allege she ever has, intends to, or intended to, sell her personal data” or that “any market for their PII other than the ‘black market’” existed); *Tate*, 2023 WL 6383467, at *5 (rejecting the plaintiffs’ allegation that the theft of their PII diminished its value, stating: “While businesses place a premium on the PII of potential customers for marketing purposes, individuals do not ordinarily reap financial gain from selling their information as a commodity.”); *Gardiner*, 2021 WL 4992539, at *3 (finding that diminution of value of personal information “can be a viable damages theory,” but only if the plaintiff “establish[es] the existence of a market for the personal information and an impairment of the ability to participate in that market,” which the plaintiff’s allegations in that case did not, as the plaintiff did not “allege that he has been unable to sell, profit from, or monetize his personal information”).

Consistent with the apparent majority of courts to consider the issue, the court finds that the allegations of the diminished value of their Private Information does not state a cognizable damages claim.

Future Harm: The Cost of Credit Monitoring and Identity Theft Monitoring

For the same reasons as those set forth above in connection with the implied contract claim, the court finds that the plaintiffs have adequately alleged facts that, if true, would entitle them to recover the reasonable and necessary cost of future credit monitoring, given the type of data stolen and the fact that, according to the plaintiffs, the information has already been published on the dark web.

Emotional Injury

The defendant argues that emotional injury is not compensable in a negligence action under Tennessee law unless the plaintiffs allege “serious” or “severe” mental injury. (Doc. No. 29 at 23 (citing *Camper v. Minor*, 915 S.W.2d 437, 446 (Tenn. 1996)).) This is not an accurate statement of the law. Rather, in Tennessee, when a plaintiff brings a stand-alone claim for negligent infliction of emotional distress, a plaintiff must prove serious mental injury. *Miller v. Willbanks*, 8 S.W.3d 607, 615 (Tenn. 1999) (citing *Camper*, 915 S.W.2d at 446). However, “in a case in which a claim for emotional injury damages is one of multiple claims for damages . . . , there is no need to impose special pleading or proof requirements that apply to ‘stand-alone’ emotional distress claims.” *Est. of Amos v. Vanderbilt Univ.*, 62 S.W.3d 133, 137 (Tenn. 2001).⁷

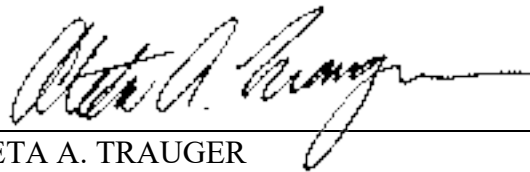
⁷ In Arkansas, where plaintiff Walker lives, damages for mental and emotional injury are not recoverable in the absence of physical injury or “willful and wanton wrongs and those committed with the intention of causing mental distress.” *FMC Corp. v. Helton*, 202 S.W.3d 490, 503 (Ark. 2005) (quoting *M.B.M. Co., Inc. v. Counce*, 596 S.W.2d 681, 684 (Ark. 1980)). In Minnesota, where plaintiff Ducrepin lives, a plaintiff may recover damages for emotional injury only where he suffers a physical injury, was within the “zone of danger” and exposed to physical harm, or suffers a “direct invasion of his rights, such as defamation, malicious prosecution, or other

The plaintiffs here do not allege serious or severe emotional injury, but they have, at least for pleading purposes, established that they may be entitled to compensatory damages to cover the cost of future credit monitoring and identity-theft monitoring. In this circumstance, the plaintiffs may be entitled to recover emotional injury along with other monetary damages.

The plaintiffs, in short, have alleged cognizable damages arising from the defendant's negligence in maintaining the security of their Private Information in the form of the expected future costs of credit monitoring and the anxiety associated with their fear of identity theft.

IV. CONCLUSION

For the reasons set forth herein, the defendant's Motion to Dismiss Plaintiffs' Consolidated Complaint (Doc. No. 28) will be denied as to the plaintiffs' negligence, negligence *per se*, and breach of implied contract claims, but granted with respect to the plaintiffs' other claims. An appropriate Order is filed herewith.



ALETA A. TRAUGER
United States District Judge

willful, wanton or malicious conduct.” *Yath v. Fairview Clinics, N.P.*, 767 N.W.2d 34, 46 (Minn. Ct. App. 2009) (citation omitted).